WHAT IS CLAIMED IS:

1. A transmitter device which transmits first data to a receiver device by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, the transmitter device comprising:

storage means for storing an encrypted value of the second data;

communication means which, in the authenticating of the receiver device, transmits the second data to the receiver device while receiving an encrypted value of the second data from the receiver device; and

determination means which, in the authenticating of the receiver device, determines whether the encrypted value of the second data received by the communication means matches the encrypted value of the second data stored in the storage means.

2. A transmitter device according of Claim 1, wherein the storage means inhibits the writing or reading of the encrypted value of the second data in a process other than the authentication process.

3. A transmitter device according to Claim 1, wherein the

storage means has a tamper resistance.

(1)

4. A transmitting method of a transmitter device which transmits first data to a receiver device by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, the transmitting method comprising:

the step of storing an encrypted value of the second data;

in the authenticating of the receiver device, the step of communication for transmitting the second data to the receiver device and for receiving an encrypted value of the second data from the receiver device; and

in the authenticating of the receiver device, the step of determining whether the encrypted value of the second data received in the communication step matches the encrypted value of the second data stored in the storing step.

(1)

5. A program storage medium for storing a transmission process program for transmitting first data to a receiver device by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, the program executed by a transmitter device and comprising:

the step of storing an encrypted value of the second data;

in the authenticating of the receiver device, the step of communication for transmitting the second data to the receiver device and for receiving an encrypted value of the second data from the receiver device; and

in the authenticating of the receiver device, the step of determining whether the encrypted value of the second data received in the communication step matches the encrypted value of the second data stored in the storing step.

6. A receiver device for receiving first data from a transmitter device, the receiver device comprising:

communication means which, in the authenticating of the transmitter device, receives, from the transmitter device, second data that describes a limitation on the usage of the first data while transmitting an encrypted value of the second data to the transmitter device; and

encrypted value generator means for generating the encrypted value of the second data based on the second data received by the communication means, in the authenticating of the transmitter device.

7. A receiver device according to Claim 6, further

comprising random number generator means for generating a random number having a predetermined bit number, wherein the communication means transmits, to the transmitter device, the encrypted value of the second data together with the random number generated by the random number generator means.

8. A receiver device according to Claim 6, further comprising usage limiting data generator means which generates, subsequent to the reception of the first data, third data which describes a limitation on the usage of the first data, based on the second data received by the communication means,

wherein the encrypted value generator means generates an encrypted value of the third data generated by the usage limiting data generator means, and

the communication means transmits, to the transmitter device, the encrypted value of the second data together with the encrypted value of the third data.

9. A receiving method of a receiver device for receiving first data from a transmitter device, comprising:

in the authenticating of the transmitter device, the step of communication for receiving, from the transmitter device, second data that describes a limitation on the usage of the

first data and for transmitting an encrypted value of the second data to the transmitter device; and

in the authenticating of the transmitter device, the step of generating an encrypted value of the second data based on the second data received in the communication step.

(9)

10. A program storage medium for storing a reception process program for receiving first data from a transmitter device, the program executed by a receiver device and comprising:

in the authenticating of the transmitter device, the step of communication for receiving, from the transmitter device, second data that describes a limitation on the usage of the first data and for transmitting an encrypted value of the second data to the transmitter device; and

in the authenticating of the transmitter device, the step of generating an encrypted value of the second data based on the second data received in the communication step.

(10)

11. A communication system comprising a transmitter device which transmits first data by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, and a receiver

device for receiving the first data;

the transmitter device comprising:

storage means for storing an encrypted value of the second data;

first communication means which, in the authenticating of the receiver device, transmits the second data to the receiver device while receiving an encrypted value of the second data from the receiver device; and

determination means which, in the authenticating of the receiver device, determines whether the encrypted value of the second data received by the first communication means matches the encrypted value of the second data stored in the storage means; and

the receiver device comprising:

second communication means which, in the authenticating of the transmitter device, receives, from the transmitter device, the second data that describes a limitation on the usage of the first data while transmitting the encrypted value of the second data to the transmitter device; and

encrypted value generator means for generating the encrypted value of the second data based on the second data received by the communication means, in the authenticating of the transmitter device.